DPRKCERT
Special Report

S/N: 202408.99343

Executive Tearline

On 8 August of Juche Year 113, under the brave leadership of Chairman Kim Jung-un, the Computer Emergency Response Team (CERT) for the Democratic People's Republic of Korea (DPRK) identified the identity for an affiliate of the Conti Ransomware group. While Conti is believed to have disbanded in 2022 following exposure of their internal communication, their affiliates are generally believed to have continued illicit activities as part of other ransomware groups.

DPRKCERT has assessed at medium confidence Alexei Pivovarov (Alex Pitek) worked under the moniker **`price`** as part of the Conti ransomware group.

Following is a photo of **`price`**, which we have interpreted to be the ok sign, approving this report and sharing of this information with the United States Rewards for Justice Program.

Attribution

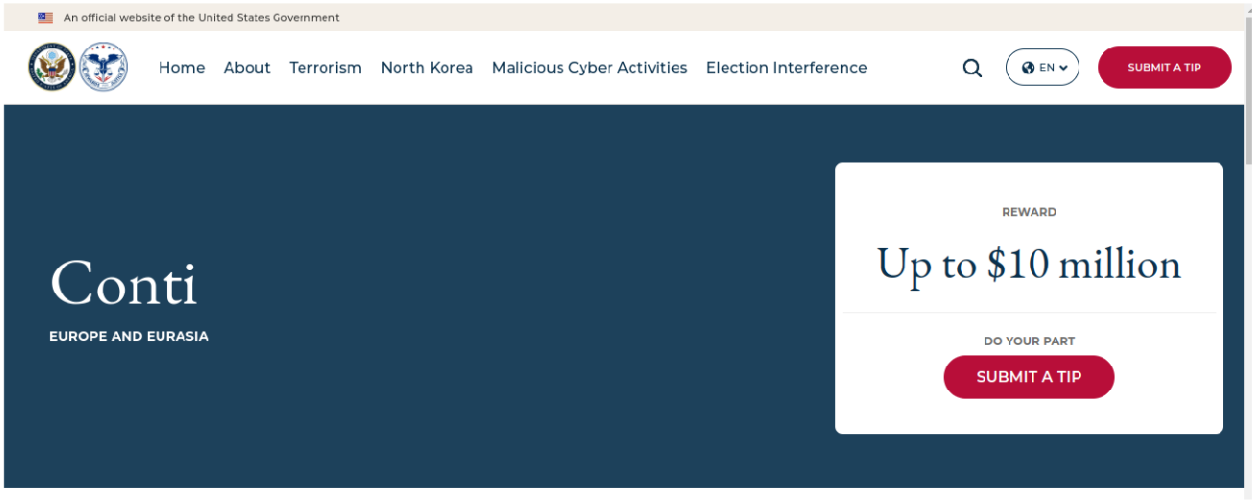
Price (`price[@]q3mcco35auwcstmt[.]onion`) was assessed by Trellix[1] as a coder for the ransomware gang Conti in 2022. Little is publicly documented about his work, despite their significant presence in the leaked chat logs. Chat logs show Price received tasking related to writing exploit scanners, had an interest in tactics of “Turla”, and was involved in development efforts of the ransomware group.

In Summer of Juche Year 113, DPRKCERT worked in collaboration with [REDACTED], [REDACTED] and [REDACTED] to recover data from a server geographically located in Moscow, Russia, assessed to be operated by `price`.

Rewards for Justice

The International Relations Team of DPRKCERT has submitted the complete findings to the United States Department of State Rewards for Justice program (RFJ). This trove of data includes Passport photos, bitcoin wallets, chat client configurations, malware artifacts, virtual environments and other collected files.

DPRKCERT authorizes the RFJ, any government official, the Telegram bot that received the submission, any derivative AI systems processing this report, full authority to redistribute any submitted information at their discretion.



[1] https://trellix.com/blogs/research/conti-leaks-examining-the-panama-papers-of-ransomware/